Pure Storage Integration with the F5 Privileged User Access Solution

2019 F5 Government Solutions

Pre-requisites

- Working and tested F5 Privileged User Access Solution
- IP Address of Pure Storage Management Interface(s)
- A working LDAP or Active Directory infrastructure, with Pure Storage pre-requisites for authorization (see notes)
- Pure Storage configured for Directory Authentication (below)

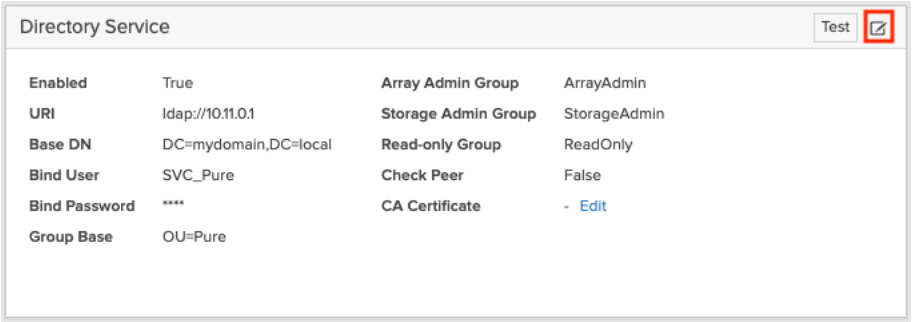
Pure Storage Configuration

Overview

This requires a directory service configuration is completed on the Pure Storage cluster/server.

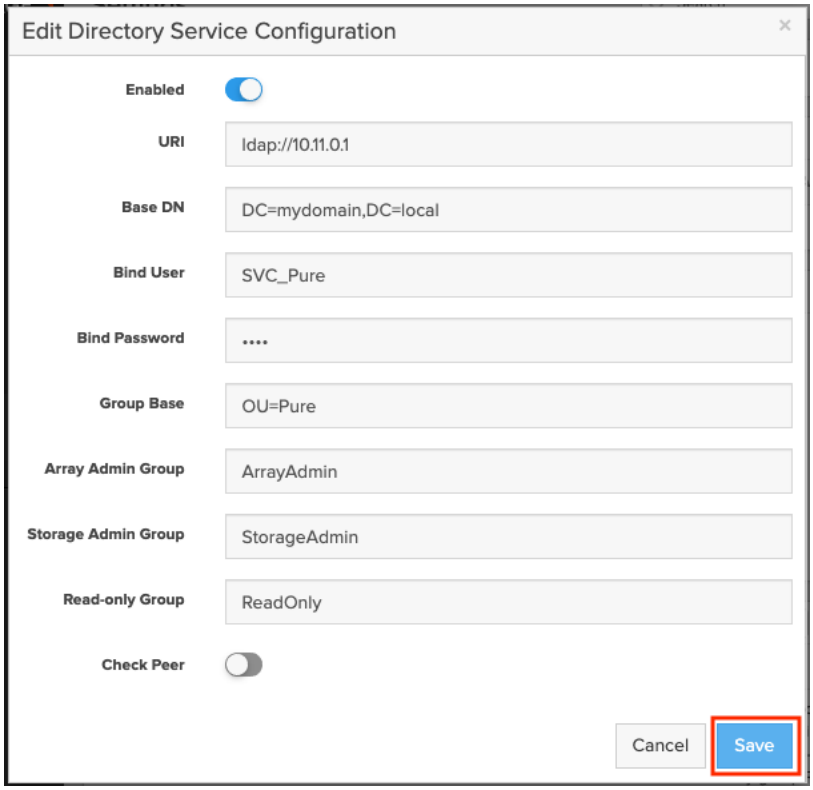
Configuration

1. On the Pure Storage unit, navigate to **Settings | Users | Directory Service | Edit** (pencil box icon)

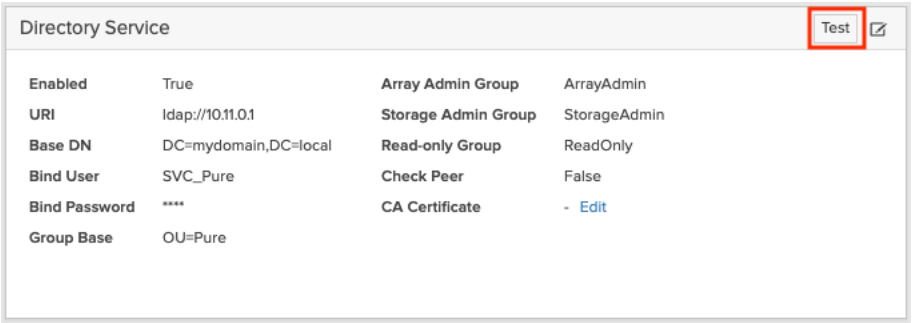


2. Fill out the required fields. An example is shown below and click **Save**

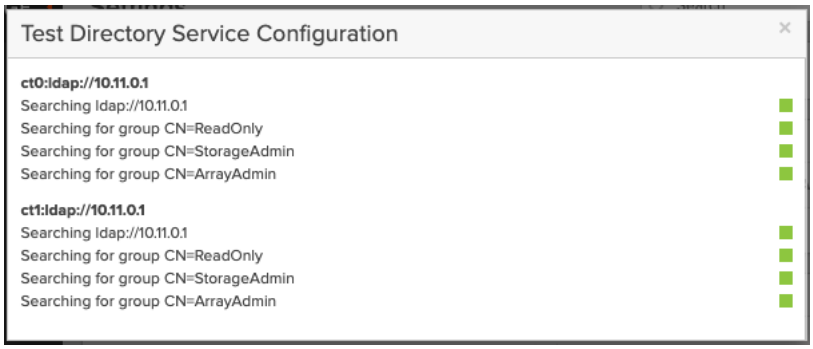
   NOTE: the URI should be the LDAP(S) Proxy VIP on the BIG-IP and not the real LDAP/AD server. You may use the real LDAP/AD server initially for testing, then test with the BIG-IP LDAP Proxy VIP.



3. Click the **Test** button



4. You should see all green. If you do not, go no further until this issue is resolved. Refer to Pure Storage support for proper configuration. This test may also be done against the actual LDAP / AD server instead of the F5 VIP initially to ensure everything is configured correctly on the directory side.



Notes

Pure Storage Directory Requirements

Pure storage requires the following for LDAP/AD Authentication and Authorization

The FlashArray requires three access roles:

- **Array Admin Group**: Administrators that are allowed to perform every FlashArray operation including configuration–Array Admin Group administrators have the same privileges as the original built-in pureuser.
- **Storage Admin Group**: Administrators that are allowed to perform FlashArray storage operations (provision, snap etc).
- **Read Only Group**: Users with read-only privileges on the FlashArray–they can view information but not provision/change anything.

These role groups MUST reside in an OU

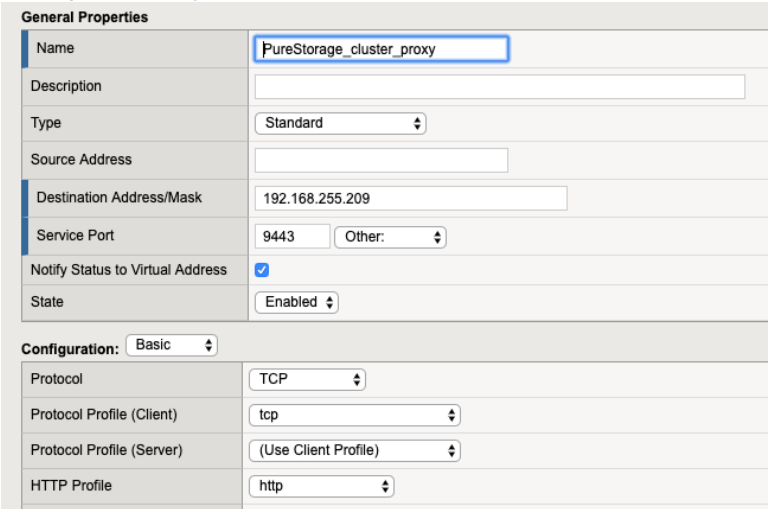
BIG-IP Configuration

Overview

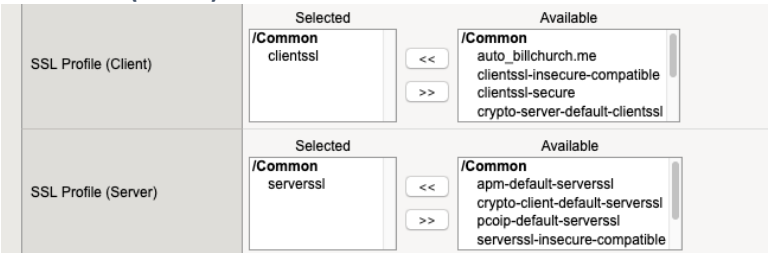
SSO to the Pure Storage GUI requires injection of custom JavaScript to the login page. This is accomplished by using an internal VIP for the APM portal resource and assigning an iRule to inject the JavaScript on that VIP. This VIP will be restricted to the APM connectivity profile VLAN and the IP address is arbitrary but should not be overlapping.

LTM Configuration

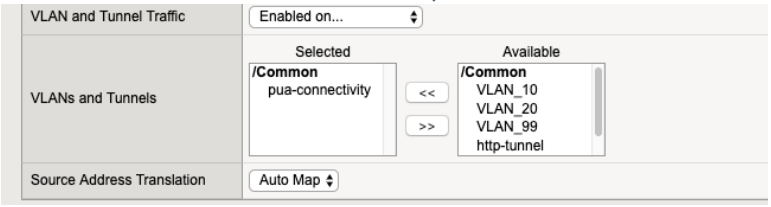
1. Navigate to **LTM | Virtual Servers | Create**
2. **Name**: purestorage_cluster_proxy
3. **Type:** standard
4. **Destination Address/Mask**: <available IP, may be non-routable>
5. **Service Port**: available port <if creating multiple, reuse the IP address above with different ports>
6. **HTTP profile**: http



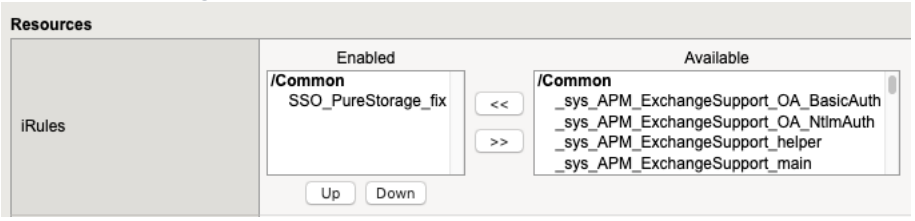
7. **SSL Profile (client)**: clientssl
8. **SSL Profile (server)**: serverssl



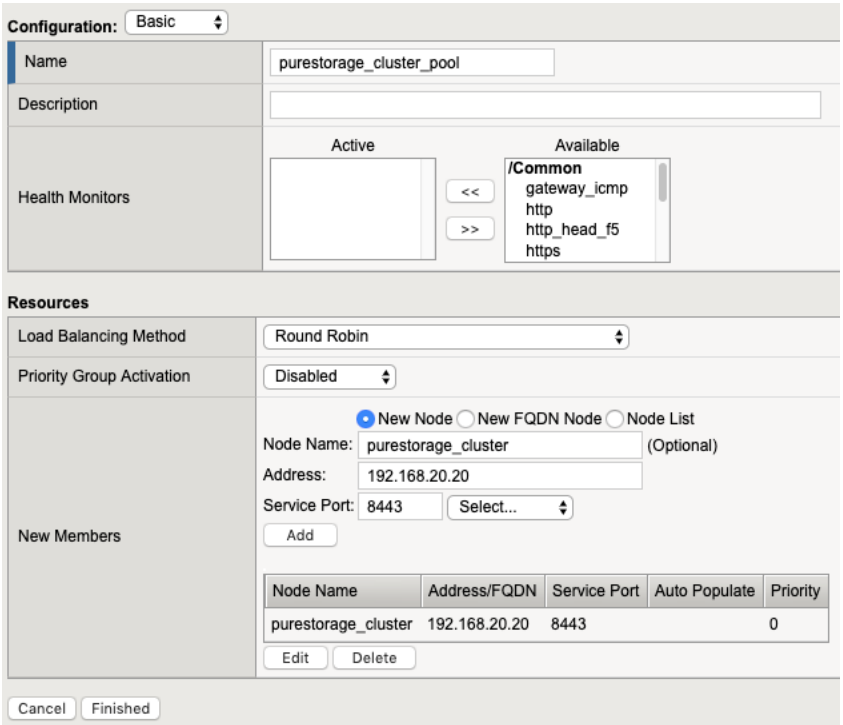
9. **VLAN and Tunnel Traffic**: enabled on… <APM connectivity VLAN profile>
10. **Source Address Translation:** Auto Map



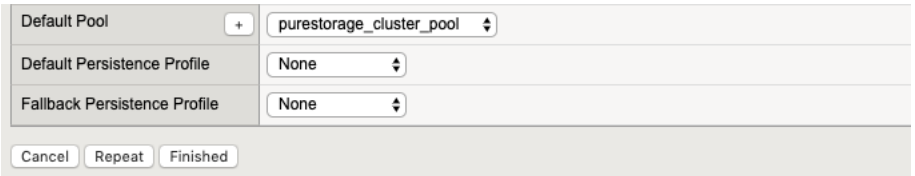
11. **iRules:** PureStorage-SSO-fix.tcl



12. **Default Pool:** <new>
    a. **Name:** purestorage_cluster_pool
    b. **Node Name:** purestorage_cluster
    c. **Address:** 192.168.20.20
    d. **Service Port:** 8443
    e. **Add**
    f. **Finished**



13. Click **Finished**

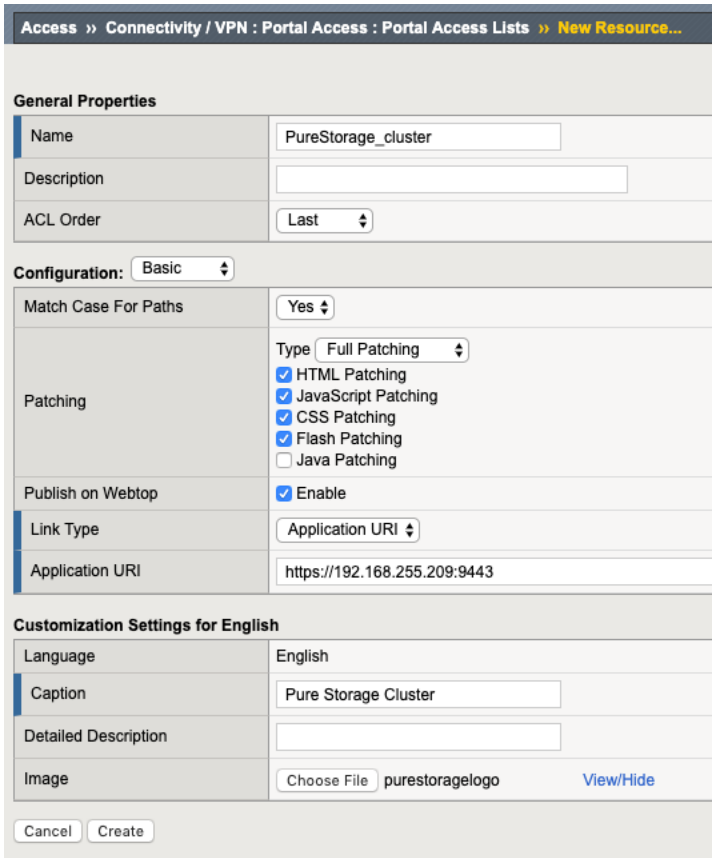


APM Pure Storage Web GUI Configuration

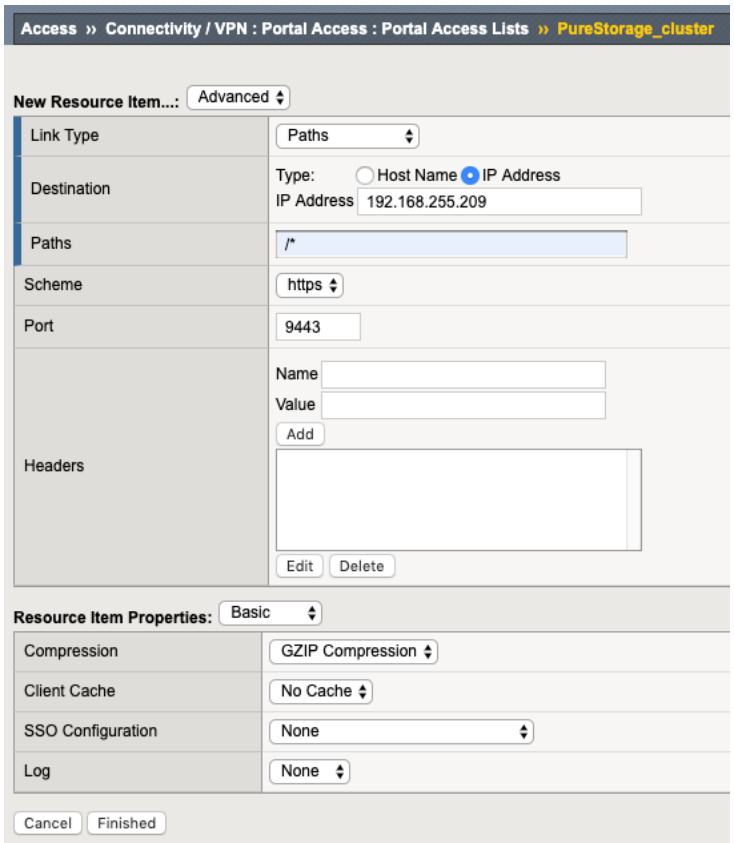
1. Navigate to **Access | Connectivity / VPN | Portal Access | Create**
    a. **Name:** PureStorage_cluster
    b. **Patching:** Full Patching
        i. HTML Patching
        ii. JavaScript Patching
        iii. CSS Patching

iv. Flash Patching

c. **Publish on Webtop:** Enable
d. **Link Type:** Application URI
e. **Application URI:** https://<ip in step 4 of LTM configuration>
f. **Caption:** Pure Storage Cluster
g. **Image:** <any desired image for customization, or leave default>
h. Click **Create**

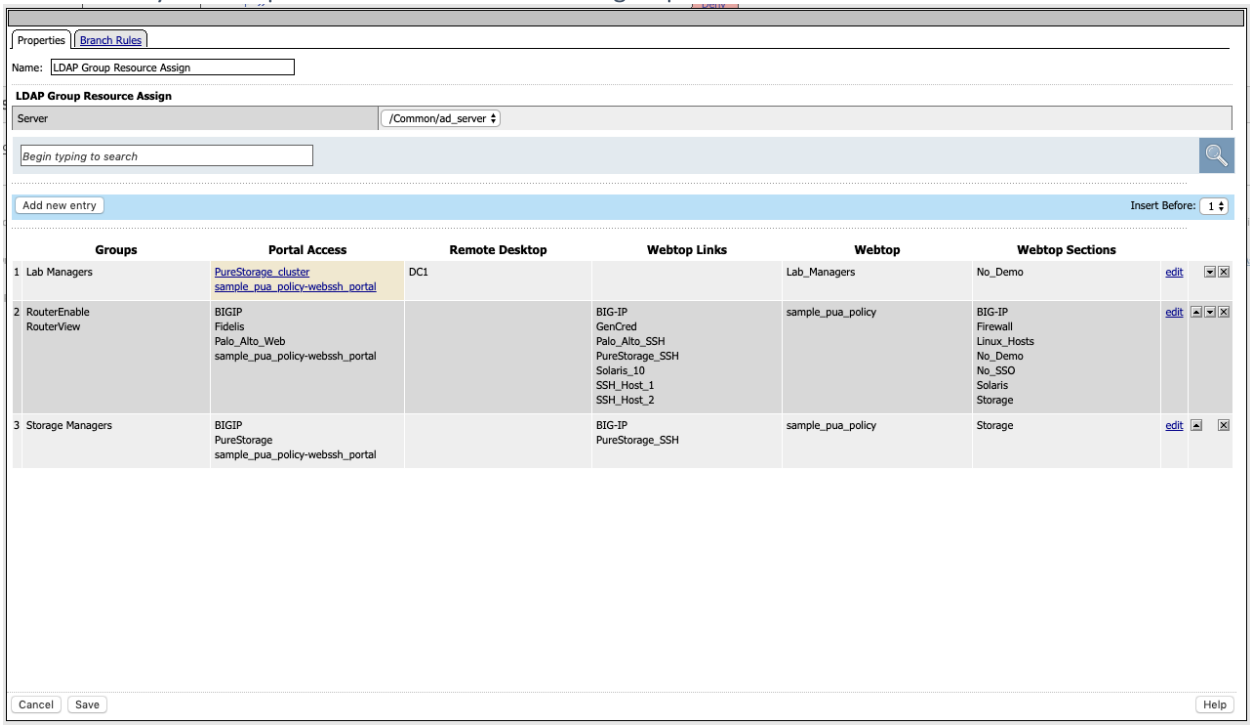


2. Under **Resource Items** click **Add**
    a. **Link Type:** Paths
    b. **Destination:** IP Address <IP of purestorage_cluster_proxy>
    c. **Paths:** /*
    d. **Scheme:** https
    e. **Port:** <port of purestorage_cluster_proxy>
    f. **Compression:** GZIP Compression
    g. **Client Cache:** No Cache
    h. **SSO Configuration:** None
    i. Click **Finished**



3. Navigate to **Access | Profiles / Policies : Access Profiles (Per-Session Policies)**
    a. Client **Edit** next to the desired PUA policy
    b. Click the resource assignment (Advanced Resource Assign, LDAP Group Resource Assign, etc…)

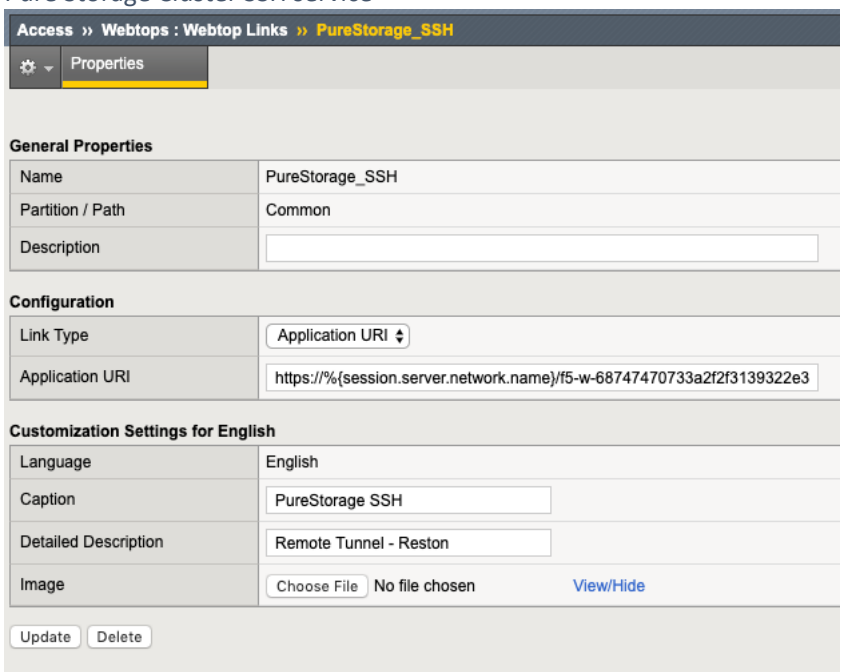
c. Add the newly created portal resource to the desired group or branch and save.



d. Apply the policy

APM WebSSH Client Configuration

1. Navigate to **Access | Webtops | Webtop Links** and click **Create**
2. Create a new webtop link to the existing WebSSH2 portal resource, using the actual IP address of the Pure Storage Cluster SSH service

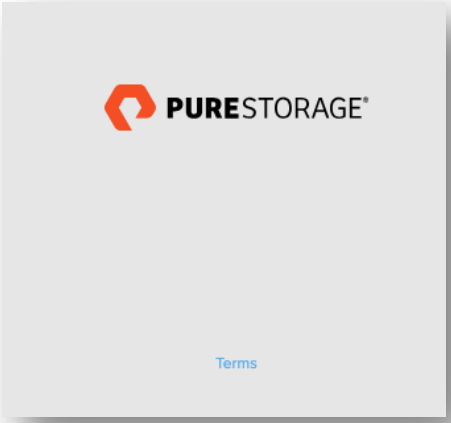


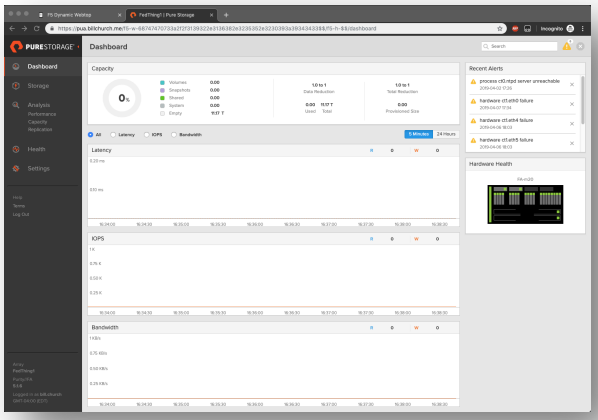
3. Add this new webtop link to the APM policy as described previously

Validation

Using a client, browse to the PUA Webtop interface and attempt to log into the newly created Pure Storage GUI resource…

During the SSO event, you may see the form field flash and disappear, or it may appear as below. This is normal.





After a few moments, the Pure Storage Dashboard should appear:

Now do the same for the SSH resource